Alex

Security Engineer / Compliance Analyst
Email: alex@madicetea.com

Summary

- **8+ years of experience** as a **cybersecurity engineer** and **compliance analyst**.
- **Work authorization**: **United States** and **Japan dual citizen**.

Key Skills and Competencies

- **Alerting**: Grafana, Prometheus, OpsGenie, ServiceNow, Slack (via API Application)
- **Cloud, Container, and Endpoint Security Monitoring**: AWS GuardDuty, CrowdStrike, Malwarebytes ThreatDown (Malwarebytes Nebula), Microsoft Defender for Cloud, Prisma Cloud, Qualys, SentinelOne, Snyk.io
- **Compliance Frameworks**: AICPA SOC 2, CIS, ISO 27001, NIST 800 (-30, -51, -61, -80, -171), NIST CSF
- **Compliance Software**: Drata, Intune, JAMF, Vanta Security, Whistic, OneTrust VRM, OneTrust QRA
- **Dashboards and Visualization**: Amazon QuickSight, Excel, Kibana, JIRA, PowerBI, Redash
- **Data Loss Protection**: Proofpoint, Fortinet NEXT, DoControl, Google Workspace for Enterprise
- **Endpoint Detection and Response**: CrowdStrike, SentinelOne, Fortinet, Microsoft Defender, Malwarebytes / ThreatDown
- **Identity & Access Management (IAM) Administration**: AWS IAM, Azure Entra, Google Workspace
- **Identity Provider (IdP) authentication**: Amazon Cognito OIDC, AWS IAM Identity Center, Azure Active Directory, Google Workspace SAML, OKTA SSO
- **Incident Detection and Pattern Recognition**: Google BigQuery SQL, Kibana, Lucerne, Splunk
- **Incident Post-Mortem [Root Cause Analysis] Report Writing**: AWS Personal Health Dashboard, Blameless
- **Script Writing**: AWS CloudShell, Azure CLI, Google Cloud CLI, Python, SQL
- **Threat Signature Trend Analysis and Writing**: Snort signature, Spamhaus DNS definitions, YARA rules

Certifications

- **AWS Certified Security – Specialty** | Obtained 2025
- **AWS Certified AI Practitioner, Cloud Practitioner, AWS Solution Architect (Associate), SysOps Administrator (Associate)** | Obtained 2024
- **CompTIA Certified ~~Security+~~, ~~Network+~~** | Obtained 2022
- **Microsoft Certified Azure System Administrator** | Obtained 2021
- **CompTIA Certified CDIA+, Mobility+, ~~A+~~** | Obtained 2017

(Next certifications: Red Hat Certified Systems Administrator RHCSA, and ISC^2 CISSP. Some COMPTIA certs expired.)

Work Experience

Security Engineer

Amazon Web Services (AWS), Amazon Inc. – *California & Washington, USA* **| June 2023 – November 2024**

- Coordinated 200 investigatory and compliance requests across **15 AWS security services**, including **AWS CloudTrail**, for **large corporate**, **government**, and **internal** clients in **Japan**, achieving a 99% resolution rate within the target SLA.
- Created and set new rules in **Fortinet NEXT DLP** to match the needs of the Enterprise Acceptable User Policy, including to protect against external generative AI use and offline corporate device data exfiltration.
- Served as the team's on-call lead **Subject Matter Expert (SME)** for **AWS Artifact**, **AWS GuardDuty**, **AWS IAM Identity Center** and **AWS Inspector**. Resolved escalated issues within 36 hours (reducing resolution time by 3 days) by making myself the security contact and communicating bilingually in English and Japanese across various teams and locations.
- Assessed AWS technologies and open-source solutions, such as **Temporary Elevated Access Management (TEAM)** and **Amazon Inspector Vulnerability Database for CVEs**, against client requirements, ensuring comprehensive protection and alignment with best practices, such as advising on how to 100% meet **CIS Benchmark standards**.
- Co-developed five granular billing and cost report actions in **AWS IAM**, providing customers with fine-grained access controls beyond default managed policies, aligning with secure architecture principles.

Information Security Administrator

Blameless, Inc. – *California, USA* **| May 2022 – January 2023**

- Architected and managed **endpoint device management** systems (**Drata** compliance monitoring, **Google Workspace DLP, JAMF** & **Intune MDM**, and **SentinelOne EDR**) across 300+ devices and 100 users to ensure 100% compliance with **AICPA SOC 2 Type 1**, **NIST 800** series, and **ISO 27001:2022** standards.
- Integrated **DoControl** into Google Workspace, Microsoft 365, Slack, Salesforce, Zoom, GitHub, and JIRA with automated security action (**SOAR**) workflows in addition to using **Google Workspace DLP** for **insider threat alerting**, and **PII exposure limitation**, which reduced time to initial response for identified security incidents by 3-6 hours.
- Configured Identity and Access Management (IAM) in **Azure Active Directory** and **Google Workspace** for 80+ employees, managing authentication mechanisms, reinforcing security protocols, and defining user access controls.
- Built **single sign-on (SSO)** integration of **Whistic third-party risk management** into our **Salesforce** tenant, giving quick access to **customer trust Pentest reports** & **OneTrust SIG-LITE questionnaires** which I wrote for **RFI / RFP** responses.
    - This expedited the pre-sales cycle by up to one week and led to a revenue increase of $25+ million in ARR.
- Composed & communicated official **public-facing status messages** for the Security team during two (2) critical **security incidents**, ensuring **GDPR** and **CCPA/CPRA** regulatory adherence.
- Established an annual **Security & Privacy Awareness program**, utilizing **KnowBe4** for training and executing semi-annual **phishing simulations**, which improved organizational phishing awareness by nearly 50% of the Organization.
- Directed a comprehensive monthly **internal audit program**, coordinating with all teams and management to mitigate organizational risk through access control audits, security **vulnerability reviews** in **Synk.io**, and audit trail monitoring. During my tenure, this led to a 25% reduction in security risks identified between my first and my last monthly audit.

Information Security Analyst

Kong, Inc. – *California, USA* **| September 2021 – May 2022**

- Led and passed a **SOC 2 Type 2 audit** with **125 controls** over an accelerated 5-week period & co-presented an **ISO 27001:2013 assessment**, enhancing customer trust and aligning policies in alignment with **NIST 800** standards.
- Integrated the **Proofpoint Data Loss Prevent (DLP)** and wrote rules to manage sensitive information in the corporate Microsoft 365 Outlook cloud and OKTA, scanning over 5,000 emails daily.
- Deployed **CrowdStrike Endpoint Detection and Response (EDR)**, **Azure Active Directory, Splunk Security Information and Event Management (SIEM)** log analysis tooling, and **Drata** for automated compliance across 600+ endpoints.
- Wrote and implemented our "Document Sharing and Security Questionnaire" policy and updated our Security Confluence wiki support page with helpful privacy and security regulation guidance, incorporating over 400 responses from the **OneTrust**-provided **SIG-LITE questionnaire** and defined an SLA of less than 5 days.
- Integrated **OKTA SAML Single Sign-On** with the **OneTrust compliance** software suite (**VRM, QRA**, and **PRA** modules).
- Authored and iteratively optimized a **JIRA change management workflow** across the Company, resulting in a 330% increase in compliant changes and improving operating efficiency by 3 hours / week.
- Collaborated with **Legal** and **Executive Management** to ensure compliance with the **Personal Information Protection Law (PIPL)**, as a responsible member for the opening of a new office location in China.
- Designed and maintained 3 monthly **JIRA visualization dashboards and filtered reports**, providing actionable insights to corporate leadership and enhancing data-driven decision-making.

Senior Security and Compliance Operations Analyst

PerimeterX, Inc. – *California, USA; Remote, USA* **| November 2019 – September 2021**

- Guided over 1000 customers regarding **HTTP data logging**, **AIO (All-In-One) Bot software** detection parameters, **JavaScript supply-chain risk** analysis, and our **integrations** with **Apache, Node.JS, Fastly, and AWS Lambda**.
- Tested efficacy of **Data Loss Prevention** features and corporate network **DNS limitation rules** in **Cisco Umbrella**.
- Designed and deployed 30 automated alerting rules using **Prometheus**, and **Grafana** for visualization.
- Automated and optimized 20 **SQL queries** with dynamic data parameters in **Redash**, leading to a 40%-75% increase in efficiency and a 250% improvement in usability for customer-facing departments. Additionally, **Redash visualizations** were used in quarterly business reports, which directly facilitated up-sell agreements of up to 550%.
- Collaborated with R&D, Product, Solutions Architecture, Customer Success, and Sales teams to develop almost one thousand AI-learning pattern detection **YARA rules** in our **rapid7 SIEM** for account takeover, card testing, and other **Indicators of Compromise (IoC)**. Presently, these rules continue to process billions of API requests each hour.

Security Researcher

Pipeline, K.K. – *Tokyo, JP* **| February 2019 – July 2019**

- Recorded 100s of observations of APAC regional **C2 server** & **DNS resolver vulnerabilities** using **Spamhaus** partner **SIEM** data, configuring secure policies, and updating **cloud-hosted containers** to enhance overall security posture.
- Architected and deployed a corporate **BIND DNS server** with **Response-Policy Zones** to support **SIEM data ingestion** and managed log visualization with **Elastic Logstash Kibana (ELK)** as part of a Proof-of-Concept for an Enterprise RFP.
- Delivered **critical production support** to three client companies, driving a notable 200% increase in upsell revenue for one client. This support involved **applying endpoint security management tools** and **optimizing client systems** for better performance and security.
- Resolved a **false-positive spam listing** issue linked to nameservers of a shared hosting provider, achieving a **recovery time objective (RTO)** of one business day. Conducted a thorough **root-cause analysis** and implemented corrective measures to restore **highly available** and reliable **email security** and website communications.
- Led cost-saving initiatives by managing **secure data destruction** and upgrading our licensing and authentication to **Azure Active Directory**.
    - These risk and compliance actions gave **operational savings** of 750,000 Japanese yen in less than 3 months.

Data Security Analyst

Junction Ltd. – *Tokyo, JP* **| October 2016 – May 2017**

- **Identified a critical security vulnerability** in an event signup form & ensured protection of millions of form responders' data by **responsibly disclosing** the issue to the signup form hosting company's security team.
- Co-authored and published the Junction Tokyo 2017 event website, leveraging expertise in **web development and security** to ensure compliance with data protection standards.
    - Developed and administered **WordPress website backends**, including the implementation of **security plugins**, **SSL/TLS certificates**, and adherence to **European and Finnish digital security regulations**.
- Collaborated with the social networking team to secure our communication channels with **multi-factor authentication (MFA)**, while also creating updates on Twitter (now X) and Slack for website and event promotion.
- Managed **network security** and **physical security** measures during the event, conducting **data forensics** and overseeing the protection of sponsor demo areas through effective security controls.

Other Roles Held

University of Tokyo	- **Faculty Development Curriculum Researcher**	| September 2018 – February 2020
	- **Remote Sensing Engineering Researcher**	| September 2018 – August 2019
	- **Professional Ethics Course Lecturer**	| September 2018 – December 2018
	- **Biology Lab Teaching Assistant**	| January 2018 – February 2018

Education

Master's degree in Information Science *(MLIS)* with concentration in Information Governance, Assurance, and Security
San Jose State University – *California, USA* **| June 2023 – December 2025**

Selected Coursework: Classification Systems, Cybersecurity, Data Cataloging, Database Management and Indexing Systems, Government Information Systems, Legal Information Resources, Information Assurance, Information Governance, Information Security Policy, SQL Programming, Statistical Research Methods

Bachelor's degree in Environmental Science with ***minors*** in Information Science & Science and Technology Studies
University of Tokyo – *Tokyo, JP* **| September 2015 – September 2019**

Selected Coursework: Android Application Development, Artificial Intelligence and Statistical Machine Learning for Engineering Students, Compilers, Computer Architecture, Database Management Systems with SQL, Deep Learning with Python, Human Impacts on Artificial Intelligence, Mathematical Modelling and Simulations with MATLAB, Neural Networks in Remote Sensing, OpenCV with C++, Operating Systems